

## CLAIMS

What is claimed is:

1           1.     A method for providing access control in a protocol stack, comprising the  
2 steps of:

- 3           (a)    receiving a request to perform an operation at a layer of the protocol stack;  
4           (b)    calling an access mediator;  
5           (c)    determining if the request is to be granted based upon a predetermined  
6 security policy by the access mediator; and  
7           (d)    providing the determination by the access mediator.

          2.     The method of claim 1, wherein the receiving step (a) comprises:  
          (a1)    receiving the request by the layer to perform the operation on an object by a  
3 subject at the layer of the protocol stack.

          3.     The method of claim 1, wherein the calling step (b) comprises:  
          (b1)    calling the access mediator by the layer.

1           4.     The method of claim 1, wherein the providing step (d) comprises:  
2           (d1)    returning the determination by the access mediator to the layer.

1           5.     The method of claim 1, wherein the receiving step (a) comprises:  
2           (a1)    receiving the request by a layer manager to perform the operation on an object

3 by a subject at the layer of the protocol stack.

1 6. The method of claim 5, wherein the layer manager interfaces with each layer  
2 of the protocol stack, wherein the layer manager handles data flow to each layer of the  
3 protocol stack.

1 7. The method of claim 1, wherein the calling step (b) comprises:

2 (b1) calling the access mediator by a layer manager.

1 8. The method of claim 7, wherein the access mediator is implemented in the  
2 layer manager.

1 9. The method of claim 1, wherein the providing step (d) comprises:

2 (d1) returning the determination by the access mediator to a layer manager.

1 10. The method of claim 1, wherein the calling step (b) further comprises:

2 (b1) passing a subject's identity, an object's identity, and a requested operation to  
3 the access mediator.

1 11. The method of claim 1, further comprising:

2 (e) allowing the operation to be performed at the layer if the determination is to  
3 grant the request.

12. The method of claim 1, further comprising:

(e) blocking the operation if the determination is to not grant the request.

13. A method for providing access control in a protocol stack, comprising the steps of:

(a) receiving a request by a layer of the protocol stack to perform an operation at the layer;

(b) calling an access mediator by the layer;

(c) determining if the request is to be granted based upon a predetermined security policy by the access mediator; and

(d) providing the determination by the access mediator to the layer.

14. A method for providing access control in a protocol stack, comprising the steps of:

(a) receiving a request by a layer manager to perform an operation at a layer of the protocol stack;

(b) calling an access mediator by the layer manager;

(c) determining if the request is to be granted based upon a predetermined security policy by the access mediator; and

(d) providing the determination by the access mediator to the layer manager.

15. A system, comprising:

2 a plurality of layers of a protocol stack; and  
3 an access mediator, wherein each layer of the protocol stack may call the access  
4 mediator to determine if a request to perform an operation at a layer of the protocol stack is  
5 to be granted.

1 16. A system, comprising:  
2 a plurality of layers of a protocol stack; and  
3 a layer manager, wherein the layer manager is interfaced with each of the plurality of  
4 stack components, wherein the layer manager comprises an access mediator, wherein layer  
5 manager may call the access mediator to determine if a request to perform an operation at a  
6 layer of the protocol stack is to be granted.

1 17. A computer readable medium with program instructions for providing access  
2 control in a protocol stack, comprising the steps of:

- 3 (a) receiving a request to perform an operation at a layer of the protocol stack;  
4 (b) calling an access mediator;  
5 (c) determining if the request is to be granted based upon a predetermined  
6 security policy by the access mediator; and  
7 (d) providing the determination by the access mediator.